#2
2-502

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of	: **Hiroyuki SUZUKI**
Filed:	: **Concurrently herewith**
For:	: **SYSTEM PROVIDING A VIRTUAL....**
Serial No.	: **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

November 29, 2001

PRIORITY CLAIM AND

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-253308** filed **August 23, 2001,** a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Linda S. Chan
Reg. No. 42,400

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.:FUJO 19.208
TELEPHONE: (212) 940-8800

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　８月２３日

出願番号
Application Number: 特願２００１－２５３３０８

出願人
Applicant(s): 富士通株式会社

２００１年１０月２６日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９３３７０

【書類名】　特許願
【整理番号】　0100036
【提出日】　平成13年 8月23日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/56
【発明の名称】　仮想私設網サービスを提供するシステム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　鈴木　浩之
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100074099
【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ
【弁理士】
【氏名又は名称】　大菅　義之
【電話番号】　03-3238-0031
【選任した代理人】
【識別番号】　100067987
【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３
【弁理士】
【氏名又は名称】　久木元　彰
【電話番号】　045-573-3683
【手数料の表示】
【予納台帳番号】　012542
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　仮想私設網サービスを提供するシステム

【特許請求の範囲】

【請求項１】　複数のルータ装置を含むＩＰ網を利用して仮想私設網サービスを提供するシステムであって、

上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とする仮想私設網サービスを提供するシステム。

【請求項２】　請求項１に記載のシステムであって、

同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有する。

【請求項３】　請求項１に記載のシステムであって、

第１のルータ装置内に設けられた第１の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第１の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルータユニットから上記第１の仮想ルータユニットへ応答情報が返送され、

上記第１の仮想ルータユニットは、上記応答情報に基づいて、対応する仮想私設網のネットワーク構成を検出する。

【請求項４】　請求項１に記載のシステムであって、

第１のルータ装置内に設けられた第１の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第１の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルー

タユニットである第２の仮想ルータユニットから上記第１の仮想ルータユニットへ応答情報が返送され、

上記第１の仮想ルータユニットと上記第２の仮想ルータユニットとの間に上記ルーティング情報を転送するための制御チャネルが設定される。

【請求項５】　ＩＰ網を利用して仮想私設網サービスを提供するシステムにおいて使用されるルータ装置であって、

上記仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とするルータ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＰ網を利用して構築される仮想私設網およびその仮想私設網のために使用されるルータ装置に係わる。

【０００２】

【従来の技術】

従来より、多くのユーザが私設網（あるいは、自営網）を構築している。私設網は、あるグループ内の端末装置間のみでのデータ転送を許可するネットワークであり、従来は、一般に、専用線を利用して構築されていた。ところが、近年では、通信コストの削減などの要求により、インターネット等の不特定多数のユーザに開放されているＩＰ網を利用して仮想的な私設網を構築しようとする動きが広がっている。なお、インターネットは、世界中のユーザに広く開放されたＩＰ網であり、多数のルータ装置により構築されている。

【０００３】

インターネット上では、データは、基本的に、ＩＰパケットに格納されて転送

される。ここで、各ＩＰパケットにはそれぞれ宛先アドレスが付与されている。そして、各ルータ装置は、ＩＰパケットを受信すると、付与されている宛先アドレスに従ってそのＩＰパケットの経路を決定する。この場合、経路の決定に際して、ルーティングテーブルが参照される。

【０００４】

ルーティングテーブルは、ＩＰパケットの転送経路を決定するための情報を含んでおり、ルーティングアルゴリズムにより設定および管理される。一例としては、宛先ネットワークとネクストホップとの対応関係を表す情報が登録されている。この場合、ルータ装置は、受信したＩＰパケットの宛先アドレスを検索キーとしてルーティングテーブルを検索することによりネクストホップを決定し、上記ＩＰパケットをそのネクストホップへ送出する。そして、経路上の各ルータ装置により上記処理が実行されることにより、ＩＰパケットが宛先アドレスへ転送される。

【０００５】

インターネット上の仮想私設網は、通常、ＩＰトンネリング（IP Tunneling）により実現される。代表的なＩＰトンネリングとしては、例えば、マイクロソフト社のＰＰＴＰ（Point-to-Point Tunneling Protocol ）や、シスコシステムズ社のＬ２Ｆ（Layer 2 Forwading ）などが知られているが、現在では、これら２つのプロトコルが融合されたＬ２ＴＰ（Layer 2 Tunneling Protocol）が普及しつつある。ここで、Ｌ２ＴＰは、ＰＰＰ（Point-to-Point Protocol ）データをトンネルしながら、データリンク層でそのパケットを暗号化するプロトコルである。なお、Ｌ２ＴＰは、ＩＥＴＦ（Internet Engineering Task Force ）により標準化されており、ＲＦＣ２６６１として制定されている。

【０００６】

【発明が解決しようとする課題】

上述のように、インターネットを利用して仮想私設網を構築する方法は、ＩＥＴＦなどにおいて検討されている。しかし、すべての仕様が議論されているわけではない。例えば、セキュリティを確保する方法については十分な議論がなされているとは言えない。

【０００７】

例えば、各ルータ装置は、現状、１つのルーティングテーブルを用いてルーティング処理を行っている。そして、そのルーティングテーブルには、一般ユーザのためのルーティング情報、および仮想私設網サービスユーザのためのルーティング情報が格納されている。すなわち、ルーティングテーブルは、不特定多数のユーザのために共通に利用されるようになっている。

【０００８】

このため、ルーティングテーブルに格納されているルーティング情報は、不正アクセスにより盗まれたり、書き換えられたりする危険性がある。すなわち、ルーティング情報が盗まれ、それを解析されると、仮想私設網サービスユーザのネットワーク構成が知られてしまう。また、ルーティング情報を書き換えることにより、特定の仮想私設網内で送受信される情報が盗聴される可能性もある。

【０００９】

また、仮想私設網を実現する方法の１つとして、ＭＰＬＳ－ＶＰＮ（Multi-Protocol Label Switching-Virtual Private Network）が知られている。しかし、この方法では、複数の拠点にそれぞれ設けられているネットワーク（例えば、キャンパスネットワーク）をＢＧＰ（Border Gateway Protocol ）などを利用して互いに接続しようとすると、各ネットワークがそれぞれ独立した自律網（ＡＳ：Autonomous System ）となってしまい、全体で１つの自律網を構築することはできない。したがって、複数のネットワークが専用線で接続されている仮想私設網を、インターネットを利用した仮想私設網に移行することは困難である。

【００１０】

本発明の目的は、ＩＰ網を利用した仮想私設網のセキュリティを向上させることである。

【００１１】

【課題を解決するための手段】

本発明の仮想私設網サービスを提供するシステムは、複数のルータ装置を含むＩＰ網を利用する方式であって、上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニット

を有し、その仮想ルータユニットが、対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段とを有する。

【００１２】

上記システムにおいては、仮想私設網ごとにルーティングテーブルが分離されている。そして、そのルーティングテーブルを利用して仮想私設網サービスが提供される。したがって、各仮想私設網のセキュリティが高い。

【００１３】

上記システムにおいて、同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有するようにしてもよい。この構成によれば、ルーティングテーブルを作成するための情報が、仮想私設網ごとに独立に送受信されるので、セキュリティがさらに向上する。

【００１４】

【発明の実施の形態】

図１は、実施形態の仮想私設網（ＶＰＮ：Virtual Private Network ）に係わるシステムの構成図である。ここでは、ユーザＡ、ユーザＢ、ユーザＣに対してそれぞれ仮想私設網サービスが提供されているものとする。

【００１５】

実施形態の仮想私設網は、ＩＰ公衆網であるインターネットを利用して構築される。ここで、ＩＰ公衆網には、多数の通信ノードが設けられており、各ユーザは、それぞれ対応するエッジノード（Edge Node ）１Ａ～１Ｄに収容される。また、各通信ノード（エッジノード１Ａ～１Ｄを含む）は、例えば、ルータ装置などの通信機器である。なお、ＩＰ公衆網を利用して構築される仮想私設網は、しばしば「ＩＰ－ＶＰＮ」と呼ばれている。

【００１６】

各ユーザ（ユーザＡ～ユーザＣ）は、それぞれ、複数のサイトに端末装置を有している。たとえば、ユーザＡは、エッジノード１Ａ～１Ｄにより管理される各

サイトにそれぞれ端末装置を有している。なお、各サイトには、端末装置が１台だけ設けられていてもよいし、複数の端末装置が接続されたＬＡＮ（Local Area Network）が設けられていてもよい。

【００１７】

仮想私設網は、擬似的に閉じたネットワークである。したがって、各仮想私設網内で送受信されるＩＰパケットは、他の仮想私設網に属する端末装置あるいは一般ユーザの端末装置に転送されることはない。また、仮想私設網内では、ＩＰパケットは、Ｌ２ＴＰなどのＩＰトンネルを利用して転送されてもよいし、ＭＰＬＳ（Multi-Protocol Label Switching）のラベルパスを利用して転送されてもよい。

【００１８】

図２は、実施形態の仮想私設網を構築する方法の概念を説明する図である。ここでは、２台のエッジノードのみを示す。なお、エッジノードは、ルータ装置であるものとする。

【００１９】

ルータ装置１０、２０は、それぞれ複数のユーザを収容することができる。ここでは、ルータ装置１０は、ユーザＡ、ユーザＢ、およびユーザＣを収容しており、ルータ装置２０は、ユーザＡおよびユーザＢを収容している。また、ルータ装置１０、２０は、それぞれ各ユーザに対応するＶＲ（Virtual Router）ポートを備えている。この実施例では、ルータ装置１０には、ユーザＡに対応するＶＲポート１１ａ、ユーザＢに対応するＶＲポート１１ｂ、およびユーザＣに対応するＶＲポート１１ｃが設けられている。同様に、ルータ装置２０には、ユーザＡに対応するＶＲポート２１ａ、およびユーザＢに対応するＶＲポート２１ｂが設けられている。なお、各ユーザと対応するＶＲポートとの間は、基本的に１：１に接続されている。

【００２０】

各ＶＲポートは、それぞれルーティングテーブルを備えている。ここで、このルーティングテーブルは、仮想私設網ごとに作成される。すなわち、ＶＲポート１１ａが備えるルーティングテーブル１２ａおよびＶＲポート２１ａが備えるル

ーティングテーブル２２ａには、ユーザＡの仮想私設網のためのルーティング情報のみが格納されている。同様に、ルーティングテーブル１２ｂ、２２ｂにはユーザＢの仮想私設網のためのルーティング情報のみが格納されており、ルーティングテーブル１２ｃにはユーザＣの仮想私設網のためのルーティング情報のみが格納されている。

【００２１】

また、各ＶＲポートは、同一の仮想私設網に属するＶＲポートのみとの間でルーティング情報などの制御情報を交換する。このとき、これらの制御情報は、Ｌ２ＴＰなどにより形成されるＩＰトンネルを介して送受信される。例えば、ＶＲポート１１ａは、ＶＲポート２１ａとの間にＬ２ＴＰトンネルを形成できるが、他のＶＲポートとの間にはそれを形成することはできない。従って、この場合、ＶＲポート１１ａのルーティングテーブル１２ａに格納されているルーティング情報は、Ｌ２ＴＰトンネルを介してＶＲポート２１ａのみに送られる。また、このとき、ＶＲポート１１ａは、ＶＲポート２１ａのルーティングテーブル２２ａに格納されているルーティング情報をＬ２ＴＰトンネルを介して受け取ることができる。そして、各ＶＲポートでは、交換されたルーティング情報により、ルーティング情報が作成／更新される。

【００２２】

なお、エッジノード間でルーティング情報を送受信する方法は、公知の技術を利用することができ、例えば、ＯＳＰＦ（Open Shortest Path First）により実現されてもよい。この場合、一方のエッジノードから他方のエッジノードへ情報が送られる際に、その経路上に設けられているルータ装置のルーティングテーブルが更新される。そして、本実施形態では、各ＶＲポートがエッジノードとして動作する。すなわち、ＶＲポート間でルーティング情報が交換され、それらのＶＲポートに設けられているルーティングテーブル、および経路上の各ルータ装置に設けられているルーティングテーブルが作成／更新される。

【００２３】

一例を示す。ここでは、ＶＲポート１１ａとＶＲポート２１ａとの間でルーティング情報が交換される場合を想定する。例えば、ＶＲポート２１ａからＶＲポ

ート１１ａへ転送されるルーティング情報は、「サイトＡ３に設けられているユーザＡの端末装置宛てのパケットは、ルータ装置２０のＶＲポート２１ａに転送される。」を含んでいる。この場合、図３に示すように、ＶＲポート１１ａのルーティングテーブル、およびＶＲポート２１ａとＶＲポート１１ａとの間の経路上に設けられている各ルータ装置のルーティングテーブルが更新される。具体的には、ルータＹのルーティングテーブルには、サイトＡ３のユーザＡ宛てのパケットをＶＲポート２１ａへ転送するための情報が登録される。また、ルータＸのルーティングテーブルには、サイトＡ３のユーザＡ宛てのパケットをルータＹへ転送するための情報が登録される。さらに、ＶＲポート１１ａのルーティングテーブル１２ａには、サイトＡ３のユーザＡ宛てのパケットをルータＸへ転送するための情報が登録される。同様に、ＶＲポート１１ａからＶＲポート２１ａへ転送されるルーティング情報は、「サイトＡ１に設けられているユーザＡの端末装置宛てのパケットは、ルータ装置１０のＶＲポート１１ａに転送される。」を含んでいる。

【００２４】

このように、実施形態のルータ装置は、仮想私設網ごとにＶＲポートを備えている。ここで、各ＶＲポートは、対応する仮想私設網のためのルーティング情報を管理しており、また、同一の仮想私設網に属するＶＲポートのみとの間でそのルーティング情報を交換する。これにより、仮想私設網ごとにルーティング情報が分離され、各仮想私設網のセキュリティが向上する。

【００２５】

仮想私設網内で送受信されるパケットのルーティング処理は、対応するＶＲポートにより行われる。例えば、サイトＡ１に設けられているユーザＡの端末装置からサイトＡ３に設けられているユーザＡの端末装置宛てのパケットが送出されると、そのパケットは、まず、ルータ装置１０のＶＲポート１１ａにより受信される。ＶＲポート１１ａは、受信したパケットの宛先きアドレスを検索キーとしてルーティングテーブル１２ａからルーティング情報を取り出し、そのルーティング情報に従って上記パケットを送出する。この場合、上記パケットは、図３に示したルーティング情報に従って、ルータＸ、ルータＹを介してＶＲポート２１

ａへ転送される。そして、ＶＲポート２１ａが、そのパケットをサイトＡ３のユーザＡへ転送する。このように、端末装置間で送受信されるパケットは、ＶＲポートにより形成される仮想私設網内を転送される。

【００２６】

なお、図３では、一般的なルーティングテーブルを示したが、ラベル付きのルーティングテーブルであっても、その作成／更新手順は基本的に同じである。

図４は、仮想私設網を提供するルーティングエリアの構造を模式的に示す図である。ルーティングエリアは、階層的な構造を有しており、制御プレーンおよびユーザプレーンから構成される。制御プレーンは、ＶＲポート間で制御情報を送受信するためのエリアである。なお、制御情報は、上述したように、仮想私設網ごとに形成されるトンネルを介して送受信されるので、仮想私設網ごとに互いに分離されている。一方、ユーザプレーンは、主信号（端末装置間で送受信されるデータ）を送受信するためのエリアである。ここで、ルータ装置は、上述したように、仮想私設網ごとに設けられるＶＲポートを備えている。また、各仮想私設網内の主信号は、対応するＶＲポートによりルーティングされる。したがって、ユーザプレーンは、仮想私設網ごとのプレーンに分離されている。

【００２７】

図５は、実施形態のルータ装置の構成図である。ここで、このルータ装置は、複数のユーザ回線および他のルータ装置に接続される局間回線を収容している。そして、各ユーザ回線は、それぞれ対応するＶＲポートに接続されている。

【００２８】

ルータ装置は、上述したように、１または複数のＶＲポート３０を備える。そして、ＶＲポート３０は、ゲートウェイプロトコルデーモン３１、ルーティングテーブル３２、制御チャネル終端部３３、ＶＰＮ構成モジュール３４、ラベル付与部３６などを備える。

【００２９】

ゲートウェイプロトコルデーモン３１は、ルータ装置の基本動作を提供する。具体的には、ルーティングテーブルを作成／更新する処理、パケットのルートを決定する処理などを実行する。なお、ゲートウェイプロトコルデーモン３１は、

例えば、ＭＰＬＳ（Multi-Protocol Label Switching）ネットワークを介してＩＰパケットを転送する機能を備える。また、ゲートウェイプロトコルデーモン３１は、プライベートアドレスとグローバルアドレスとを相互に変換する機能を備えていてもよい。

【００３０】

ルーティングテーブル３２には、対応する仮想私設網のためのルーティング情報が格納される。ここで、ルーティングテーブル３２は、所定のルーティングアルゴリズムにより設定／管理される。一例としては、図６(a) に示すように、宛先ネットワークとネクストホップの組合せが登録されている。この場合、ルータ装置（ＶＲポート）は、受信したＩＰパケットの宛先アドレスを検索キーとしてルーティングテーブルを検索することによりネクストホップを決定し、上記ＩＰパケットをそのネクストホップへ送出する。なお、ルーティングテーブルの構造は、特に限定されるものではない。

【００３１】

制御チャネル終端部３３は、ＶＲポート間で制御情報（ルーティング情報等）を伝送するための制御チャネルを終端する。ここで、制御チャネルは、Ｌ２ＴＰトンネルにより実現される。したがって、制御チャネル終端部３３は、Ｌ２ＴＰクライアントおよびＬ２ＴＰサーバを備える。Ｌ２ＴＰクライアントは、Ｌ２ＴＰトンネルの設定を要求するプログラムユニットである。一方、Ｌ２ＴＰサーバは、Ｌ２ＴＰクライアントからの要求に従ってＬ２ＴＰトンネルを形成するプログラムユニットである。

【００３２】

ＶＰＮ構成モジュール３４は、上記制御チャネルが設定されるときに、その制御チャネルに接続されるＶＲポートを認証する。このため、ＶＰＮ構成モジュール３４は、ＲＡＤＩＵＳクライアントおよびＲＡＤＩＵＳサーバを備える。ＲＡＤＩＵＳクライアントは、ＶＲポートの認証を要求するプログラムユニットである。一方、ＲＡＤＩＵＳサーバは、ＲＡＤＩＵＳクライアントからの要求に従ってＶＲポートを認証するプログラムユニットである。

【００３３】

また、ＶＰＮ構成モジュール３４は、上記制御チャネルを監視／制御する機能を備える。具体的には、例えば、定期的に制御チャネルを介して監視メッセージを送出し、対応するＶＲポートから応答メッセージを受信できるか否かをモニタする。そして、応答メッセージを受信できなかったときに、その制御チャネルを削除する処理などを行う。

【００３４】

さらに、ＶＰＮ構成モジュール３４は、対応する仮想私設網の構成を定義するＶＰＮ構成マップ３６を作成する。ＶＰＮ構成マップ３６は、少なくとも、対応する仮想私設網に係わるルータ装置を識別するルータＩＤのリストを含む。ここで、「仮想私設網に係わるルータ装置」とは、その仮想私設網に属する端末装置を収容するルータ装置のことをいう。また、ＶＰＮ構成マップ３６は、図６(b)に示すように、その端末装置を収容するＶＲポートのＩＰアドレスが登録される構成であってもよい。

【００３５】

ラベル付与部３６は、ＭＰＬＳのラベルスイッチのためのラベルをＩＰパケットに付与する。なお、ラベルスイッチは、公知の技術であり、例えば、タグスイッチ（ＲＦＣ２１０５）や、セルスイッチルータ（ＲＦＣ２０９８）などが知られている。

【００３６】

ラベルマトリクス３７は、ＶＲポートから出力されたＩＰパケットをラベルに従って対応する局間回線に導く。また、局間回線から入力されたＩＰパケットをラベルに対応するＶＲポートに導く。

【００３７】

このように、実施形態のシステムでは、主信号（端末装置間で送受信されるデータ）はＭＰＬＳネットワークを介して伝送される。しかし、ＭＰＬＳのラベルパスは、仮想私設網ごとに設けられたＶＲポートにより設定される。このため、各ラベルパスは、仮想私設網ごとにＶＲポート内で閉じている。したがって、仮想私設網内のユーザデータが盗聴されることはない。

【００３８】

図７は、ＶＲポートが増設される際のシーケンスを説明する図である。ここでは、ユーザＡの仮想私設網（以下、仮想私設網Ａ）のために、ＶＲポート（A1）およびＶＲポート（A2）が既に設けられているものとする。そして、この仮想私設網を拡張するために、ＶＲポート（A3）が追加（増設）されるものとする。

【００３９】

なお、各ＶＲポートには、それぞれ対応する仮想私設網を識別するＶＰＮ識別子が付与されている。例えば、ＶＲポート（A1）～（A3）には、それぞれ仮想私設網Ａを識別するＶＰＮ識別子が付与されている。また、各ＶＲポートには、それぞれＩＰアドレスが割り当てられている。

【００４０】

この場合、まず、ＶＲポート（A3）は、すべてのルータ装置に対して増設メッセージをブロードキャストする。この増設メッセージは、仮想私設網Ａを識別するＶＰＮ識別子、ＶＲポート（A3）を収容するルータ装置を識別するルータ識別子、およびＶＲポート（A3）に割り当てられているＩＰアドレスを含んでいる。そして、この増設メッセージは、各ルータ装置の各ＶＲポートによって受信される。

【００４１】

ＶＲポート（A1）およびＶＲポート（A2）は、増設メッセージを受信すると、対応する応答（ＡＣＫ）メッセージをＶＲポート（A3）へ返送する。この応答メッセージには、増設メッセージと同様に、ＶＰＮ識別子、ルータ識別子および当該ＶＰポートのＩＰアドレスを含んでいる。なお、仮想私設網Ａを識別するＶＰＮ識別子が付与されていないＶＲポートは、上記増設メッセージを受信しても、応答メッセージを返送しない。図７に示す例では、ＶＲポート（Ｂ）は、応答メッセージを返送しない。

【００４２】

ＶＲポート（A3）は、受信した応答メッセージに基づいて、仮想私設網Ａの構成を表すＶＰＮ構成マップを作成する。この実施例では、仮想私設網ＡにＶＲポート（A1）およびＶＲポート（A2）が属していることが認識され、その認識結果に対応するＶＰＮ構成マップが作成される。

【００４３】

続いて、ＶＲポート（A3）とＶＲポート（A1）との間、及びＶＲポート（A3）とＶＲポート（A2）との間にそれぞれＬ２ＴＰトンネルが設定される。そして、それらのＬ２ＴＰトンネルを介して、それぞれルーティング情報が交換される。これにより、ＶＲポート（A3）において、ルーティングテーブルが作成される。一方、ＶＲポート（A1）およびＶＲポート（A2）では、それぞれルーティングテーブルが更新される。

【００４４】

このように、新たなＶＲポートが追加されると、その新たなＶＲポートと既存のＶＲポートとの間でルーティング情報が交換され、ルーティングテーブルが作成／更新される。ここで、ルーティング情報の交換は、同じ仮想私設網に属するＶＲポートの間で行われる。しかも、そのルーティング情報は、それらのＶＲポート間に設定されるＬ２ＴＰトンネルを介して転送される。したがって、各仮想私設網のセキュリティは高い。

【００４５】

図８は、新たに追加されたＶＲポートにおいてルーティングテーブルを作成する処理のフローチャートである。以下では、図７に示したシーケンスを参照しながら説明する。すなわち、図７に示したシーケンスにおけるＶＲポート（A3）の動作を説明する。

【００４６】

ステップＳ１では、増設メッセージをすべてのルータ装置にブロードキャストする。この増設メッセージは、上述したように、仮想私設網Ａを識別するＶＰＮ識別子、ＶＲポート（A3）を収容するルータ装置を識別するルータ識別子、およびＶＲポート（A3）に割り当てられているＩＰアドレスを含んでいる。

【００４７】

ステップＳ２では、ステップＳ１で送出した増設メッセージに対応する応答メッセージを受信する。なお、この応答メッセージは、仮想私設網Ａに属するＶＲポートのみから返送されてくる。

【００４８】

ステップＳ３では、受信した応答メッセージから必要な情報を取得する。具体的には、応答メッセージを送出したＶＲポートのＩＰアドレス、およびそのＶＲポートを収容するユーザ装置のルータ識別子などを取得する。

【００４９】

ステップＳ４では、ステップＳ３で取得した情報に基づいてＶＰＮ構成マップを作成する。このＶＰＮ構成マップは、仮想私設網Ａの構成を表し、一例としては図６(b) に示した通りである。

【００５０】

ステップＳ５～Ｓ９の処理は、応答メッセージを送出した各ＶＲポートについてそれぞれ実行される。図７に示す例では、ＶＲポート（A1）およびＶＲポート（A2）についてそれぞれ実行される。以下では、ＶＲポート（A1）について実行する場合を説明する。

【００５１】

ステップＳ５では、ＶＲポート（A1）との間にＬ２ＴＰトンネルを設定するために、Ｌ２ＴＰクライアントおよびＲＡＤＩＵＳクライアントが起動される。このとき、ＶＲポート（A3）を認証するために必要な情報がＶＲポート（A1）に送られる。そして、ＶＲポート（A1）においてＶＲポート（A3）の認証が成功すると、ＶＲポート（A3）とＶＲポート（A1）との間にＬ２ＴＰトンネルが設定される。この場合、このＬ２ＴＰトンネルを識別するトンネル識別子が決定され、以降、ＶＲポート（A3）およびＶＲポート（A1）によりそのトンネル識別子がそれぞれ管理される。なお、上記認証に失敗した場合には、処理を終了する（ステップＳ６）。

【００５２】

ステップＳ７では、ステップＳ５において設定したＬ２ＴＰトンネルを利用して、ＶＲポート（A1）との間でルーティング情報を交換する。具体的には、ＶＲポート（A1）のルーティングテーブルに格納されているルーティング情報を取得する。また、ＶＲポート（A3）が既にルーティングテーブルを備えている場合には、そのテーブルに格納されているルーティング情報をＶＲポート（A1）へ送信する。

【００５３】

ステップＳ８では、ルーティングテーブルを作成し、ステップＳ７で受信したルーティング情報をそのテーブルに登録する。なお、この時点で既にルーティングテーブルが作成されている場合には、受信したルーティング情報によりそのテーブルが更新される。この後、ステップＳ９において、未処理のＶＲポートが残ってないかがチェックされ、残っていた場合にはステップＳ５に戻る。

【００５４】

図９は、新たなＶＲポートが追加されたときの既設のＶＲポートの動作を説明するフローチャートである。以下では、図７に示したＶＲポート（A1）、ＶＲポート（A2）、またはＶＲポート（Ｂ）の動作を説明する。

【００５５】

ステップＳ１１では、ＶＲポート（A3）から増設メッセージを受信する。この増設メッセージは、上述した通りである。

ステップＳ１２では、当該ＶＲポートが属する仮想私設網を識別するＶＰＮ識別子と、受信した増設メッセージに設定されているＶＰＮ識別子とを比較する。そして、それらが一致すれば、仮想私設網Ａの中でＶＲポートが増設されたものとみなし、ステップＳ１３へ進む。一方、それらが互いに一致しなかった場合には、処理を終了する。

【００５６】

ステップＳ１３では、受信した増設メッセージから必要な情報を取得する。具体的には、増設メッセージを送出したＶＲポートのＩＰアドレス、およびそのＶＲポートを収容するユーザ装置のルータ識別子などを取得する。そして、ステップＳ１４において、応答メッセージを作成し、それをＶＲポート（A3）へ返送する。

【００５７】

ステップＳ１５では、要求されたＬ２ＴＰトンネルを設定するために、Ｌ２ＴＰサーバおよびＲＡＤＩＵＳサーバが起動される。なお、この処理は、Ｌ２ＴＰクライアントからのセットアップ要求およびＲＡＤＩＵＳクライアントからの認証要求を受信したときに実行される。この実施例では、ＶＲポート（A3）を認証

する旨の要求を受信する。

【００５８】

ＶＲポート（A3）の認証に成功した場合は、ステップＳ１７～Ｓ１９の処理が実行され、失敗した場合は、ステップＳ２１において、対応するエラー処理が実行される。

【００５９】

ステップＳ１７では、ステップＳ１３で取得した情報に基づいてＶＰＮ構成マップを作成する。このＶＰＮ構成マップは、仮想私設網Ａの構成を表し、一例としては図６(b) に示した通りである。

【００６０】

ステップＳ１８では、ステップＳ１５において設定したＬ２ＴＰトンネルを利用して、ＶＲポート（A3）との間でルーティング情報を交換する。具体的には、当該ＶＲポートのルーティングテーブルに格納されているルーティング情報をＶＲポート（A3）へ送信する。また、ＶＲポート（A3）が既にルーティングテーブルを備えている場合には、そのテーブルに格納されているルーティング情報を受け取る。そして、ステップＳ１９において、ステップＳ１８で受信したルーティング情報によりルーティングテーブルを更新する。

【００６１】

このように、仮想私設網を拡張するためにＶＲポートが追加されると、そのＶＲポートと当該仮想私設網に属する他のＶＲポートとの間にＩＰトンネルが設定される。そして、そのＩＰトンネルを介してルーティング情報が送受信される。したがって、各ルータ装置において、仮想私設網ごとにルーティングテーブルが作成される。これにより、仮想私設網のセキュリティが向上する。

【００６２】

なお、上述の実施例では、ＶＲポート間でルーティング情報を転送するためのＩＰトンネルとしてＬ２ＴＰトンネルが使用されているが、これに限定されるものではない。また、上述の実施例では、認証プロトコルとしてＲＡＤＩＵＳが使用されているが、これに限定されるものではない。さらに、上述の実施例では、既設のＶＲポートが新たに追加されたＶＲポートを認証する方式であるが、既設

のＶＲポートおよび新たに追加されたＶＲポートが相互に認証する方式であってもよい。

【００６３】

次に、ＶＲポートが削除された場合の処理を説明する。仮想私設網を縮小する場合には、対応するＶＲポートが削除される。例えば、複数のＬＡＮがＩＰ網を利用して接続されている仮想私設網において、あるＬＡＮを廃止または切り離す場合には、そのＬＡＮに対応するＶＲポートが削除される。この場合、残されたＶＲポートは、削除されたＶＲポートとの間に設定されているＬ２ＴＰトンネルを消滅させたり、ルーティングテーブルを更新したりする必要がある。

【００６４】

図１０は、あるＶＲポートが削除されたときに残されたＶＲポートの処理を示すフローチャートである。ここでは、図７～図９の手順により、同一仮想私設網内のＶＲポート間にルーティング情報を転送するためのＬ２ＴＰトンネルが設定されているものとする。また、このフローチャートの処理は、定期的に実行されるものとする。

【００６５】

ステップＳ３１では、Ｌ２ＴＰトンネルの状態を監視する。Ｌ２ＴＰトンネルの状態は、例えば、そのトンネルに接続される一方のＶＲポートから他方のＶＲポートに監視メッセージを送出し、それに対応する応答メッセージが返送されてくるか否かにより判断される。そして、監視メッセージを送出したＶＲポートが対応する応答メッセージを受信できたときは、Ｌ２ＴＰトンネルが正常であると判断される。なお、複数のＬ２ＴＰトンネルが設定されている場合は、各トンネルについて同様の処理が行われる。

【００６６】

Ｌ２ＴＰトンネルが正常でなかった場合は、ステップＳ３２において、対向するＶＲポートが削除された可能性があるものと判断し、ステップＳ３３以降の処理が実行される。

【００６７】

ステップＳ３３では、タイマが起動される。ステップＳ３４及びＳ３５では、

上記タイマの起動開始から所定時間（例えば、２４時間）内に、対向するＶＲポートが復旧したか否かを調べる。対向するＶＲポートが復旧したか否かは、上述の監視メッセージを使用して判断することができる。そして、所定時間内に対向するＶＲポートが復旧した場合には、タイマが解除され、処理が終了する。

【００６８】

一方、所定時間内に対向するＶＲポートが復旧しなかった場合には、ステップＳ３６において、上記ＶＲポートとの間に設定されている制御チャネル（Ｌ２ＴＰトンネル）を削除する。制御チャネルの削除に際しては、例えば、Ｌ２ＴＰトンネルを規定する各種パラメータが解放される。

【００６９】

ステップＳ３７では、ＶＰＮ構成マップを更新する。具体的には、ＶＰＮ構成マップから、削除されたＶＲポートに係わる情報を削除する。続いて、ステップＳ３８では、同一仮想私設網に属する残されたＶＲポート間で、ルーティング情報を交換する。そして、ステップＳ３９において、交換されたルーティング情報によりルーティングテーブルが更新される。

【００７０】

このように、ある仮想私設網に属するＶＲポートが削除されると、その仮想私設網に属する他のＶＲポートにおいて、削除されたＶＲポートに接続されていた制御チャネルが削除される。そして、残されたＶＲポートにおいて、必要に応じてルーティングテーブルが更新される。

【００７１】

図１１および図１２は、仮想私設網の構築例を示す図である。図１１に示す例では、仮想私設網サービスを受けるユーザは、複数の営業拠点を持つ私企業である。そして、ユーザごとに、各営業拠点に設けられているキャンパスネットワークが仮想私設網により互いに接続されている。

【００７２】

図１２に示す例では、仮想私設網サービスを受けるユーザは、複数のアクセスポイントを持つＩＳＰ（Internet Service Provider ）である。そして、ＩＳＰごとに、仮想私設網が構築されている。

【００７３】

なお、本発明において、「ルーティング情報」は、ＩＰ層のルーティングプロトコルで転送される情報に限定されず、ＩＰパケットのルートを決定するための情報をすべて含むものとする。例えば、「ルーティング情報」は、ＭＰＬＳのラベルパスを設定するための情報を含む。なお、ラベルパスの設定は、例えば、ＬＤＰ（Label Distribution Protocol ）により実現することができる。

【００７４】

図１３は、ＶＲポート間でラベルパスを設定する手順の例である。ここでは、図３に示したケースと同様に、ＶＲポート１１ａとＶＲポート２１ａとの間でラベルパスのためのルーティング情報が交換される場合を想定する。例えば、ＶＲポート２１ａからＶＲポート１１ａへ転送されるルーティング情報は、「サイトＡ３に設けられているユーザＡの端末装置宛てのパケットは、ラベルＦである」を含んでいる。この場合、この情報を受け取ったルータＸは、「サイトＡ３に設けられているユーザＡの端末装置宛てのパケットは、ラベルＥである」を含むルーティング情報をＶＲポート１１ａへ送る。これにより、ＶＲポート１１ａおよびルータＸでは、それぞれ図１３に示すようなテーブルが作成される。

【００７５】

なお、これらのルーティング情報は、上述の実施例と同様に、ＶＲポート１１ａとＶＲポート２１ａとの間に設定されたＩＰトンネルを介して転送される。

上記テーブルが作成された後、サイトＡ１に設けられているユーザＡの端末装置からサイトＡ３に設けられているユーザＡの端末装置宛てのパケットが送出されると、そのパケットは、まずルータ装置１０のＶＲポート１１ａにより受信される。ＶＲポート１１ａは、そのパケットに「ラベルＥ」を付与してルータＸへ送出する。ルータＸは、そのパケットを受け取ると、ラベルを「Ｅ」から「Ｆ」に書き換えた後、そのパケットをＶＲポート２１ａへ送出する。そして、ＶＲポート２１ａが、そのパケットをサイトＡ３のユーザＡへ転送する。

【００７６】

（付記１）複数のルータ装置を含むＩＰ網を利用して仮想私設網サービスを提供するシステムであって、

上記仮想私設網サービスのユーザを収容するルータ装置は、その仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とする仮想私設網サービスを提供するシステム。

【００７７】

（付記２）付記１に記載のシステムであって、

同一の仮想私設網に属する仮想ルータユニット間に上記ルーティング情報を転送するための制御チャネルを設定する設定手段をさらに有する。

【００７８】

（付記３）付記２に記載のシステムであって、

上記制御チャネルは、ＩＰトンネルである。

（付記４）付記１に記載のシステムであって、

第１のルータ装置内に設けられた第１の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第１の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルータユニットから上記第１の仮想ルータユニットへ応答情報が返送され、

上記第１の仮想ルータユニットは、上記応答情報に基づいて、対応する仮想私設網のネットワーク構成を検出する。

【００７９】

（付記５）付記１に記載のシステムであって、

第１のルータ装置内に設けられた第１の仮想ルータユニットに対応する仮想私設網を識別する識別情報が、その第１の仮想ルータユニットから他のルータ装置へブロードキャストされ、

上記識別情報により識別される仮想私設網と同じ仮想私設網に属する仮想ルー

タユニットである第２の仮想ルータユニットから上記第１の仮想ルータユニットへ応答情報が返送され、

上記第１の仮想ルータユニットと上記第２の仮想ルータユニットとの間に上記ルーティング情報を転送するための制御チャネルが設定される。

【００８０】

（付記６）付記５に記載のシステムであって、

上記第１の仮想ルータユニットは、当該第１の仮想ルータユニットの認証を要求する認証クライアント手段を有し、

上記第２の仮想ルータユニットは、上記認証クライアントからの要求に応じて上記第１の仮想ルータユニットの認証を実行する認証サーバ手段を有する。

【００８１】

（付記７）付記２に記載のシステムであって、

ある仮想私設網に属する複数の仮想ルータユニットの中の１つが削除されたときに、その削除された仮想ルータユニットに接続されていた制御チャネルが削除され、さらに残された仮想ルータユニットにおいて上記仮想私設網のネットワーク構成を表す構成マップが更新される。

【００８２】

（付記８）付記７に記載のシステムであって、

上記制御チャネルが削除されてから所定時間が経過した後に上記構成マップが更新される。

【００８３】

（付記９）ＩＰ網を利用して仮想私設網サービスを提供するシステムにおいて使用されるルータ装置であって、

上記仮想私設網サービスのユーザ毎に対応する仮想ルータユニットを有し、

その仮想ルータユニットが、

対応するユーザのパケットを転送するためのルーティング情報を格納するルーティングテーブルと、

上記ルーティングテーブルを参照して対応するユーザのパケットの転送を制御するルーティング手段と

を有することを特徴とするルータ装置。

【００８４】

【発明の効果】

本発明によれば、仮想私設網ごとにルーティングテーブルが作成されるので、各仮想私設網のセキュリティが向上する。

【図面の簡単な説明】

【図１】

実施形態の仮想私設網に係わるシステムの構成図である。

【図２】

実施形態の仮想私設網を構築する方法の概念を説明する図である。

【図３】

ルーティングテーブルの更新の一例を示す図である。

【図４】

仮想私設網を提供するルーティングエリアの構造を模式的に示す図である。

【図５】

実施形態のルータ装置の構成図である。

【図６】

(a) はルーティングテーブルの例、(b) はＶＰＮ構成マップの例である。

【図７】

ＶＲポートが増設される際のシーケンスを説明する図である。

【図８】

新たに追加されたＶＲポートにおいてルーティングテーブルを作成する処理のフローチャートである。

【図９】

新たなＶＲポートが追加されたときの既設のＶＲポートの動作を説明するフローチャートである。

【図１０】

あるＶＲポートが削除されたときに残されたＶＲポートの処理を示すフローチャートである。

【図１１】

仮想私設網の構築例（その１）である。

【図１２】

仮想私設網の構築例（その２）である。

【図１３】

ＶＲポート間でラベルパスを設定する手順の例である。

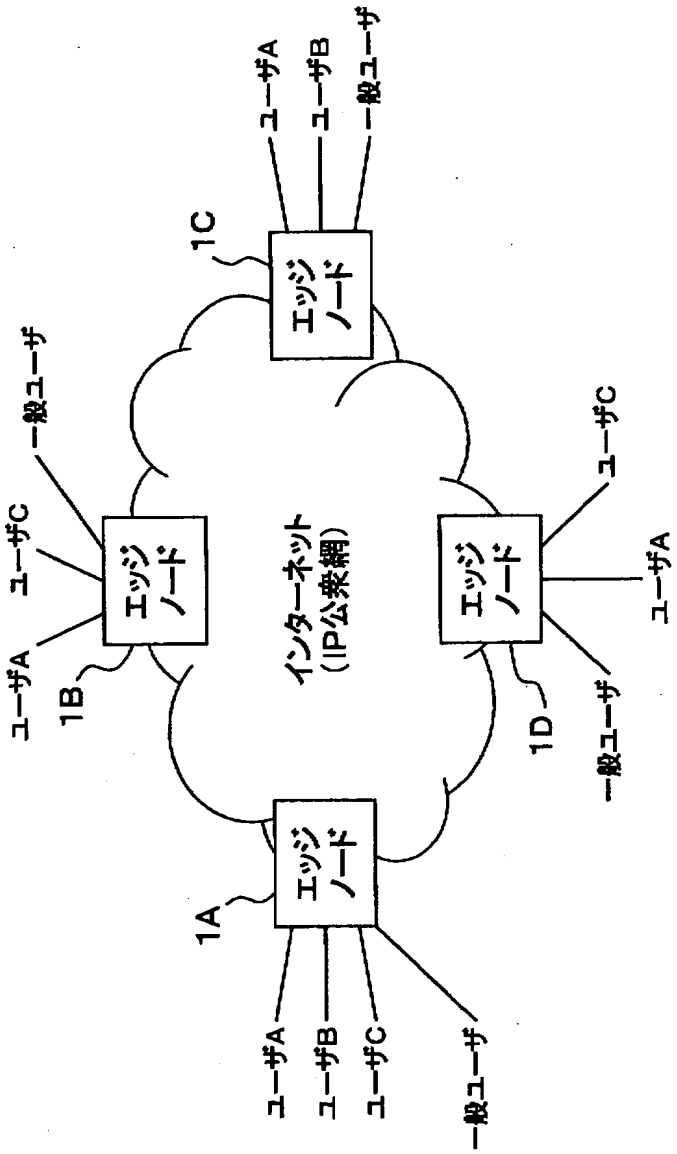
【符号の説明】

１Ａ～１Ｄ	エッジノード
１０、２０	ルータ装置
１１ａ～１１ｃ	ＶＲポート
１２ａ～１２ｃ	ルーティングテーブル
２１ａ～２１ｂ	ＶＲポート
２２ａ～２２ｂ	ルーティングテーブル
３０	ＶＲポート
３１	ゲートウェイプロトコルデーモン
３２	ルーティングテーブル
３３	制御チャネル終端部
３４	ＶＰＮ構成モジュール
３５	ＶＰＮ構成マップ

【書類名】　　図面

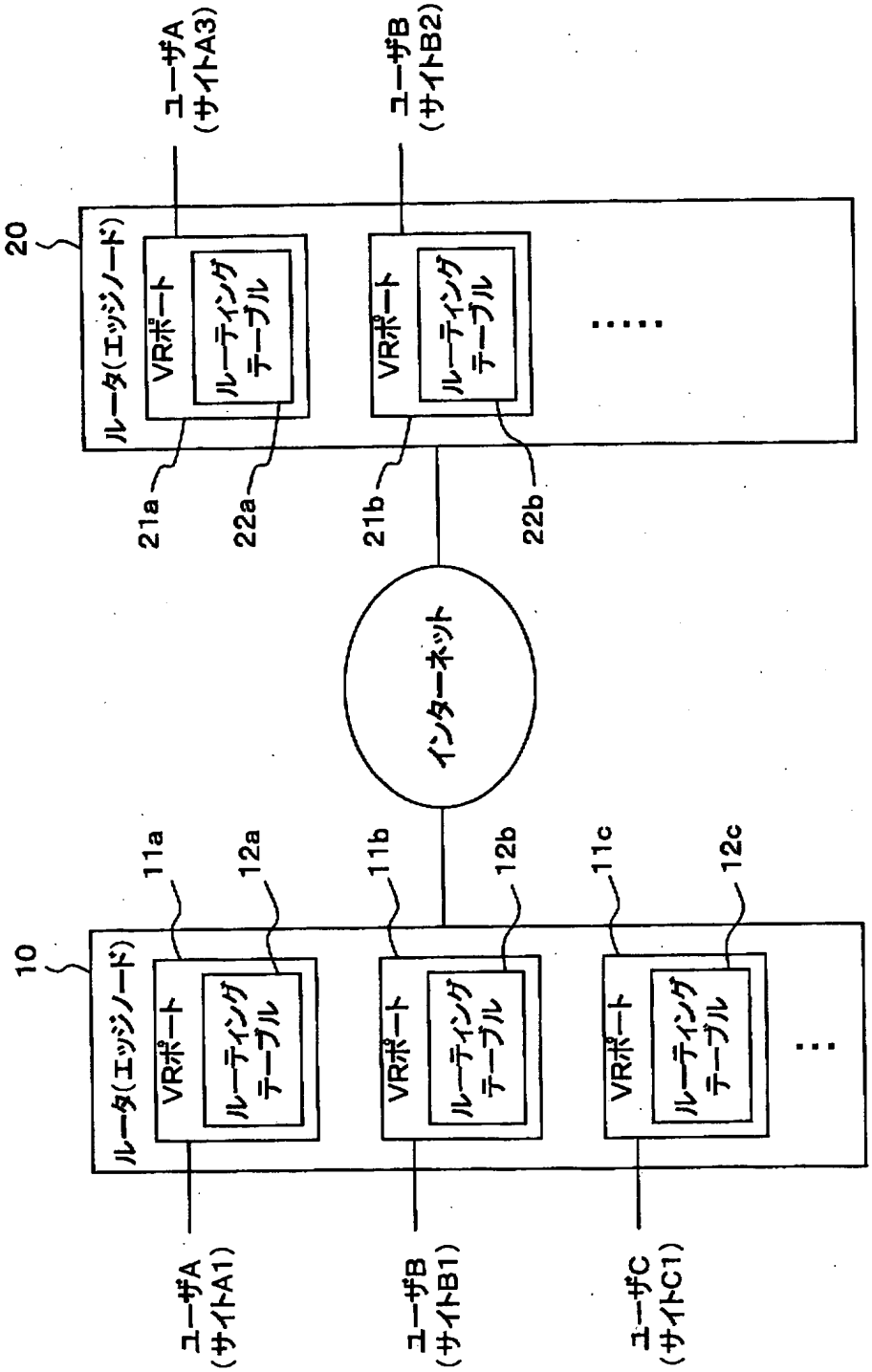
【図１】

実施形態の仮想私設網に係わるシステムの構成図



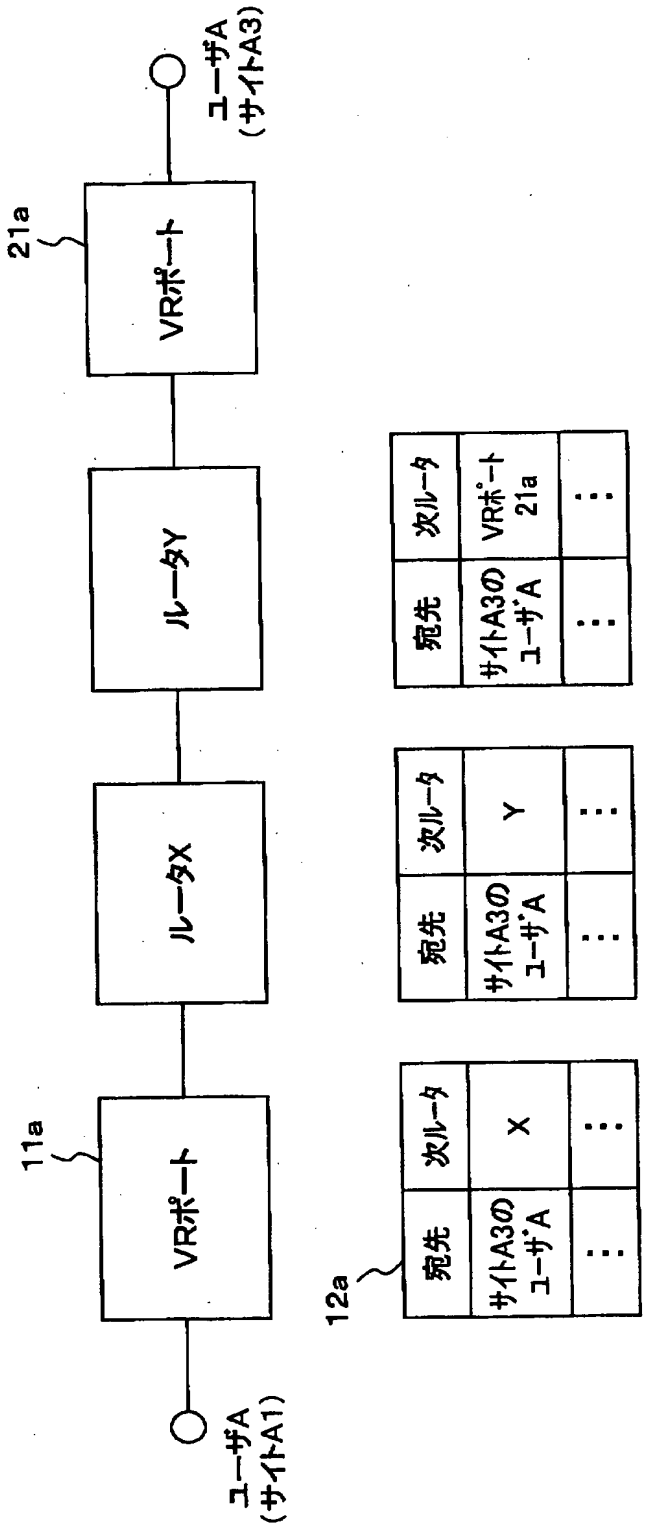
【図２】

実施形態の仮想私設網を構築する方法の概念を説明する図



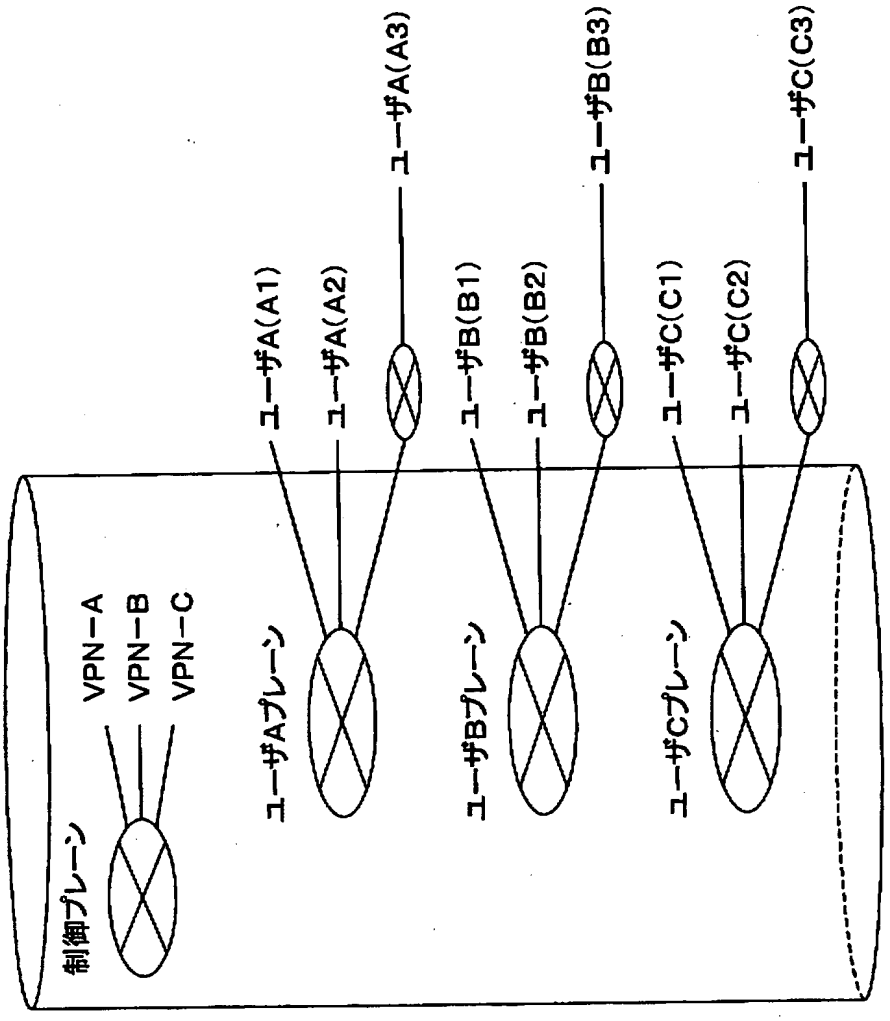
【図３】

ルーティングテーブルの更新の一例を示す図



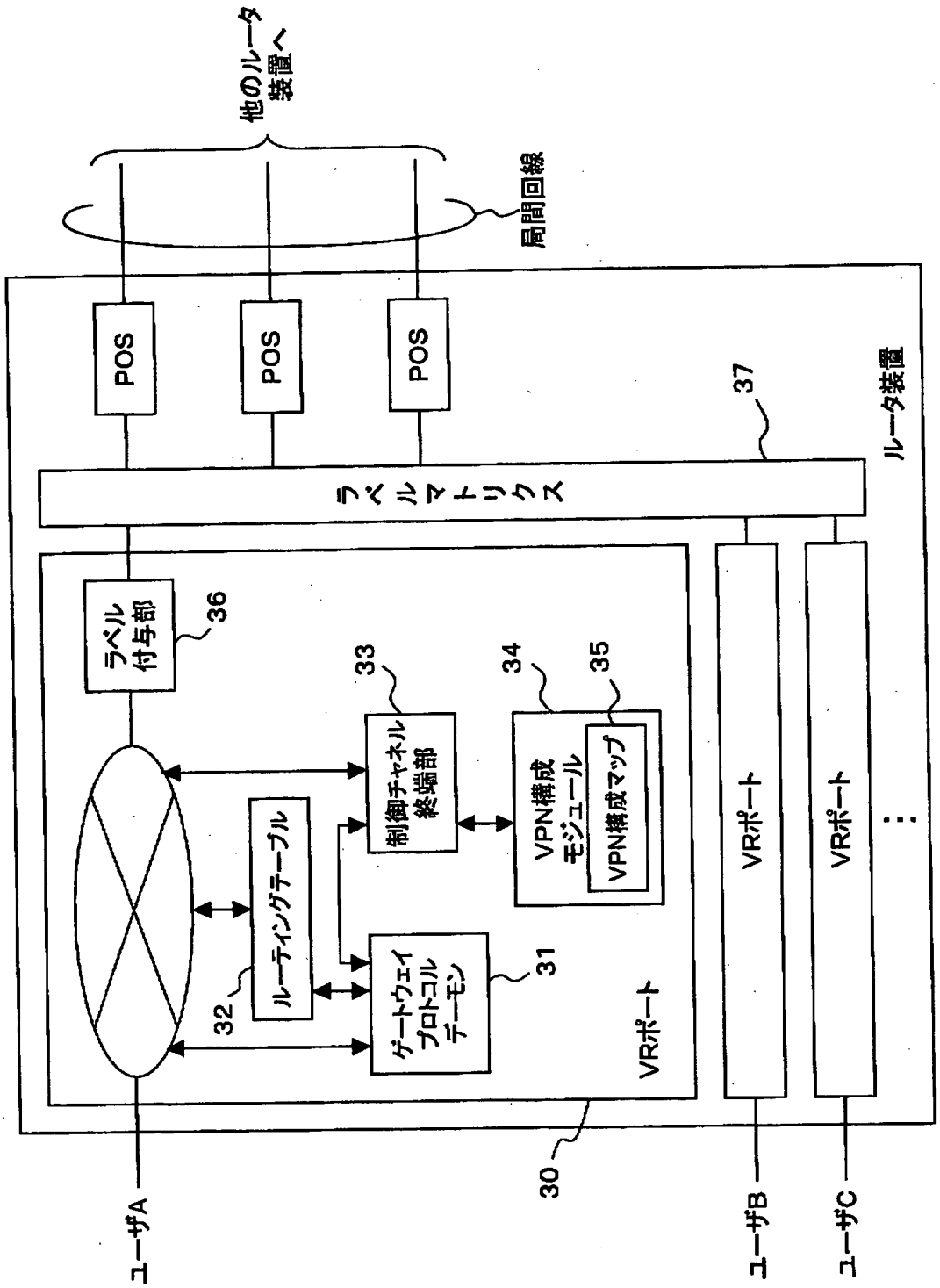
【図４】

仮想私設網を提供するルーティングエリアの
構造を模式的に示す図



【図５】

実施形態のルータ装置の構成図



【図６】

(a) はルーティングテーブルの例、(b) はVPN構成マップの例

(a)

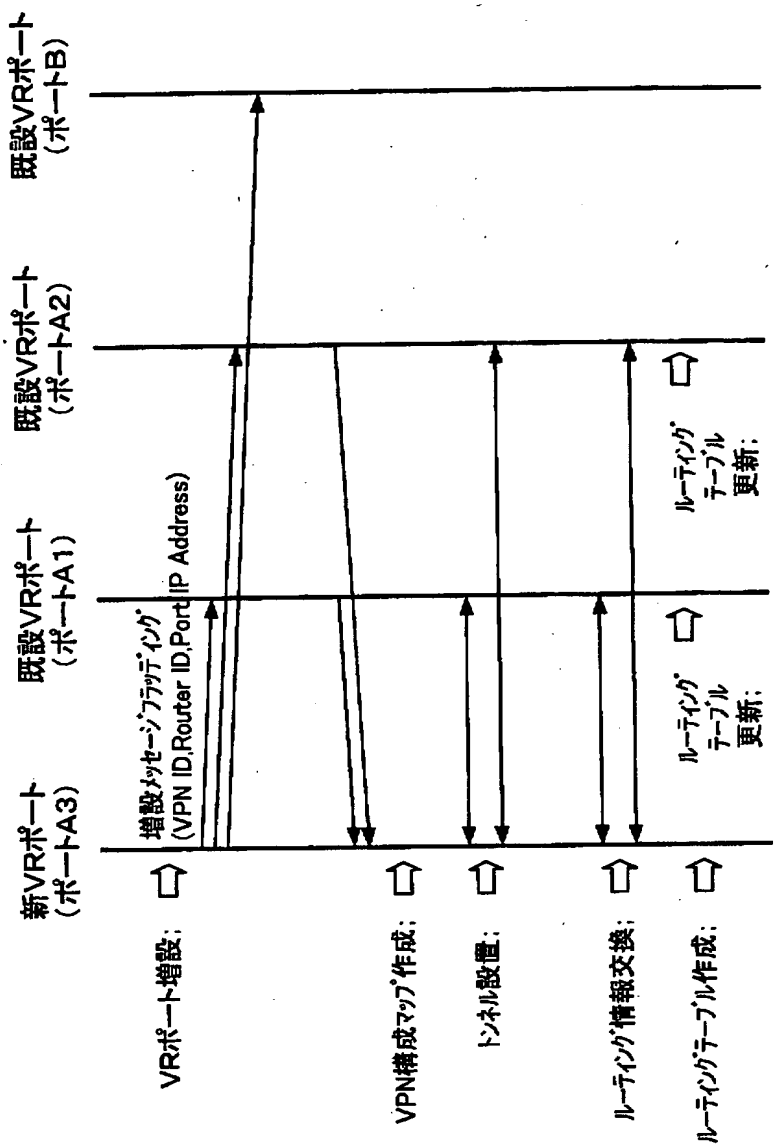
宛先ネットワーク	ネクストホップ
13	ノードA
52	ノードC
14	ノードA
27	ノードB
28	ノードB
⋮	⋮

(b)

ルータID	IPアドレス
1053	アドレスabc
0022	アドレスxyz
0134	アドレスaax
⋮	⋮

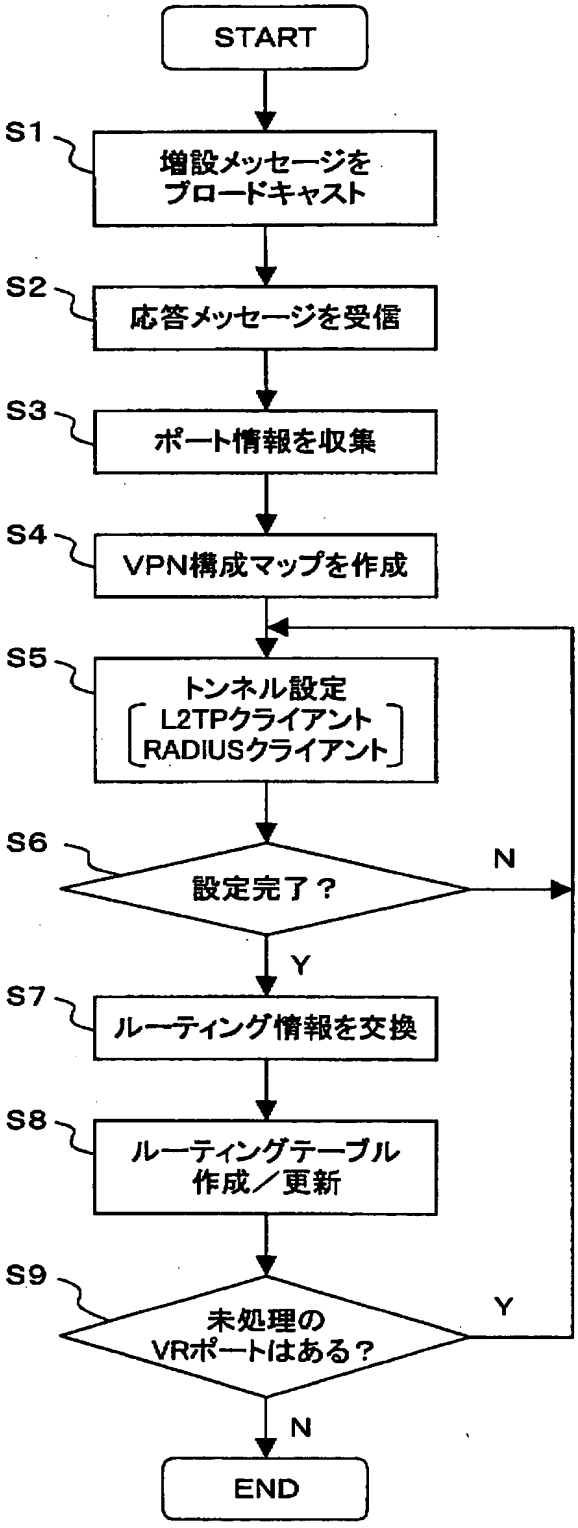
【図７】

VRポートが増設される際のシーケンスを説明する図



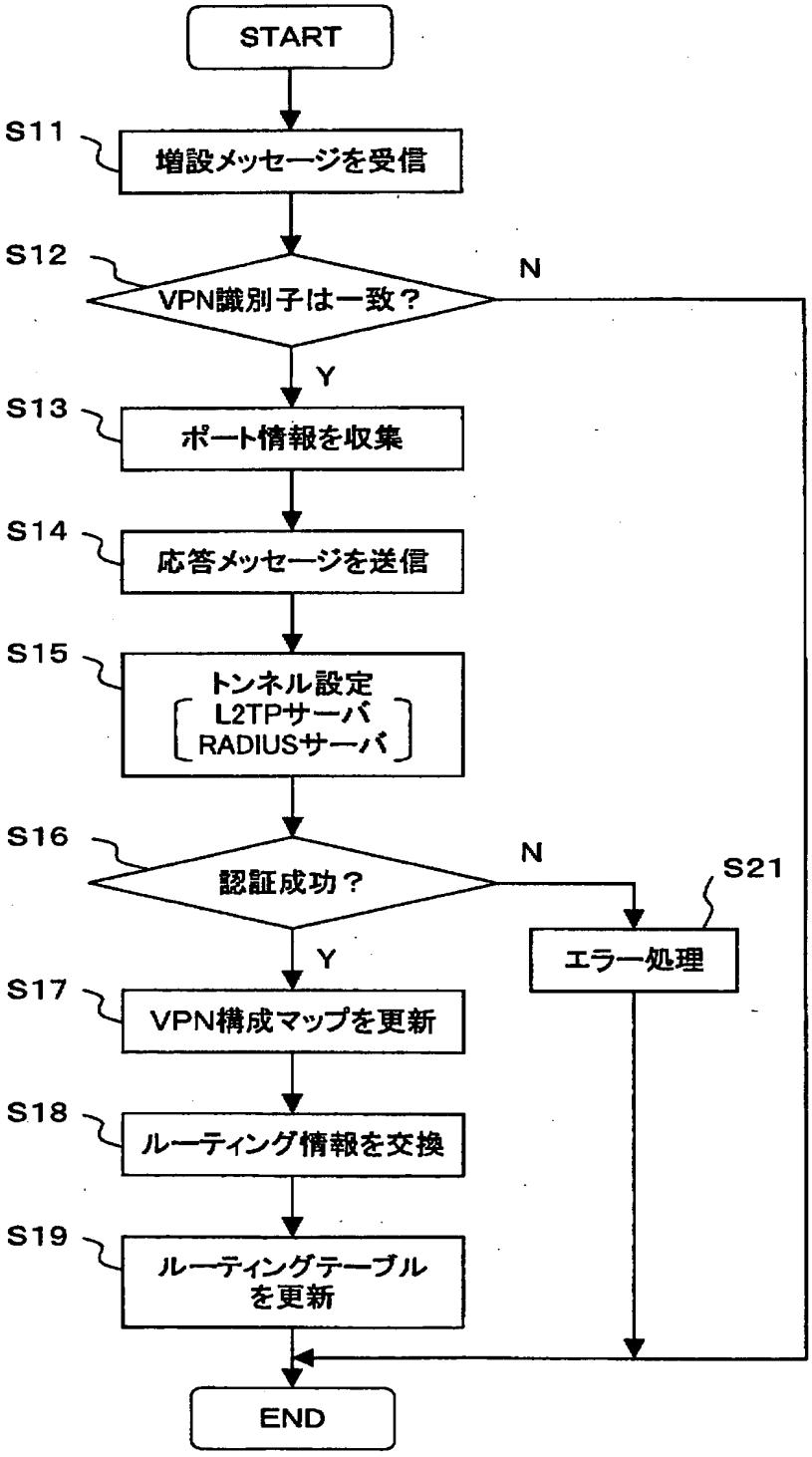
【図８】

新たに追加されたVRポートにおいてルーティングテーブルを作成する処理のフローチャート



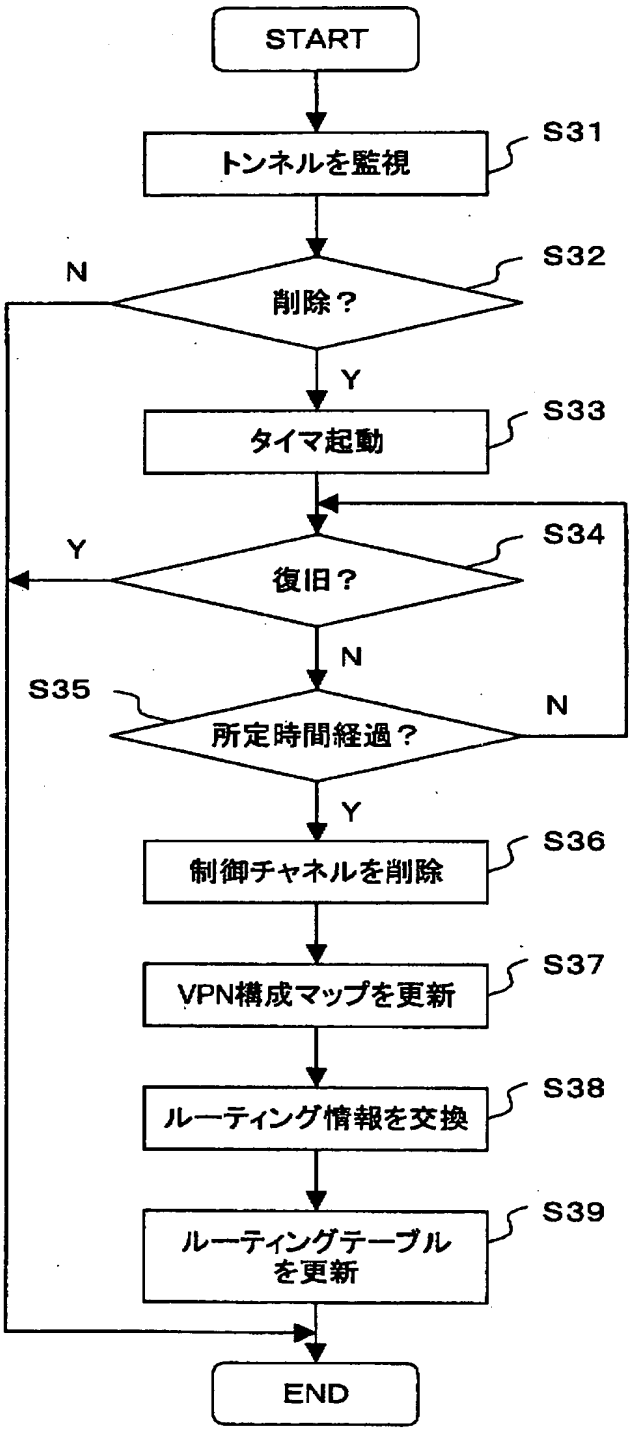
【図９】

新たなVRポートが追加されたときの既設のVRポートの動作を説明するフローチャート



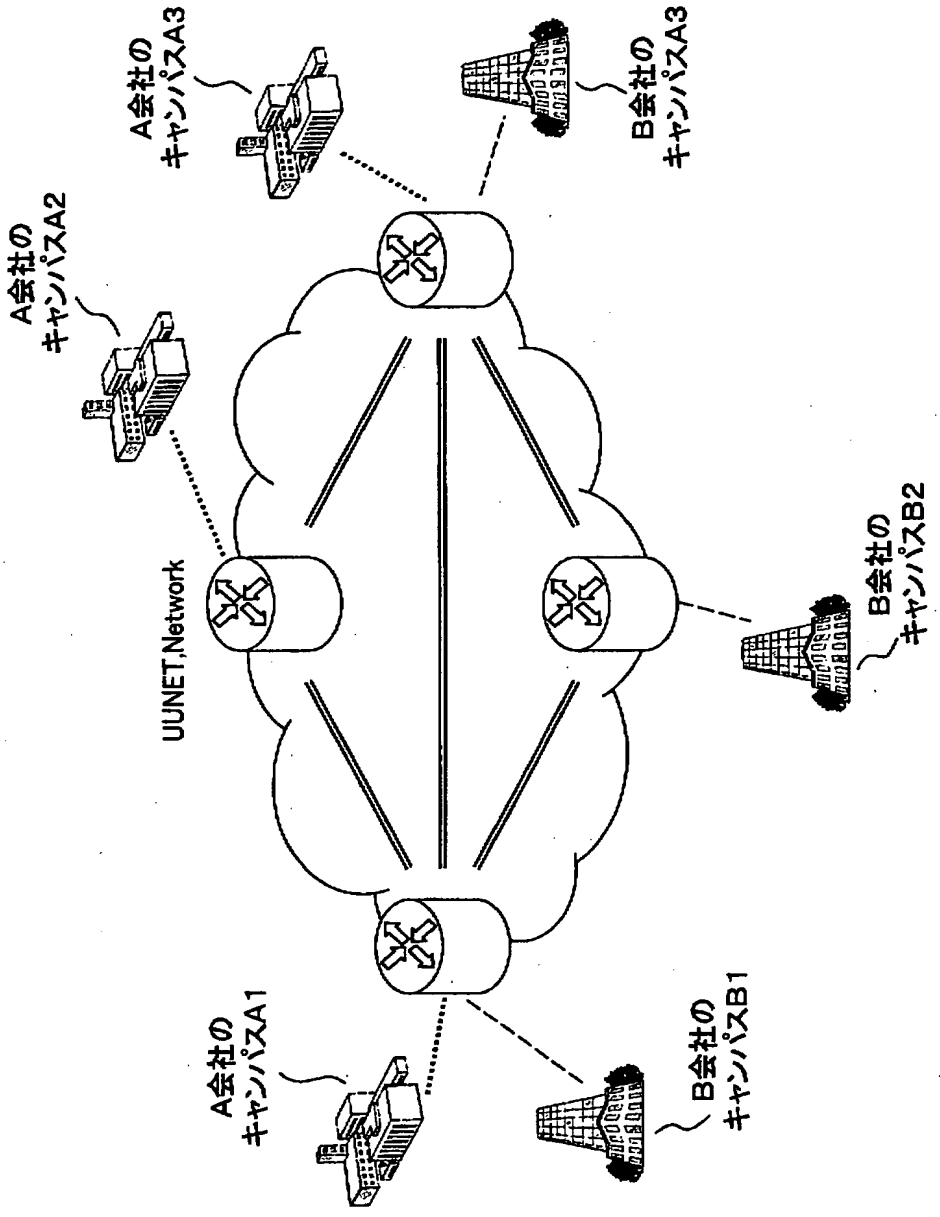
【図１０】

あるVRポートが削除されたときに残されたVRポートの処理を示すフローチャート



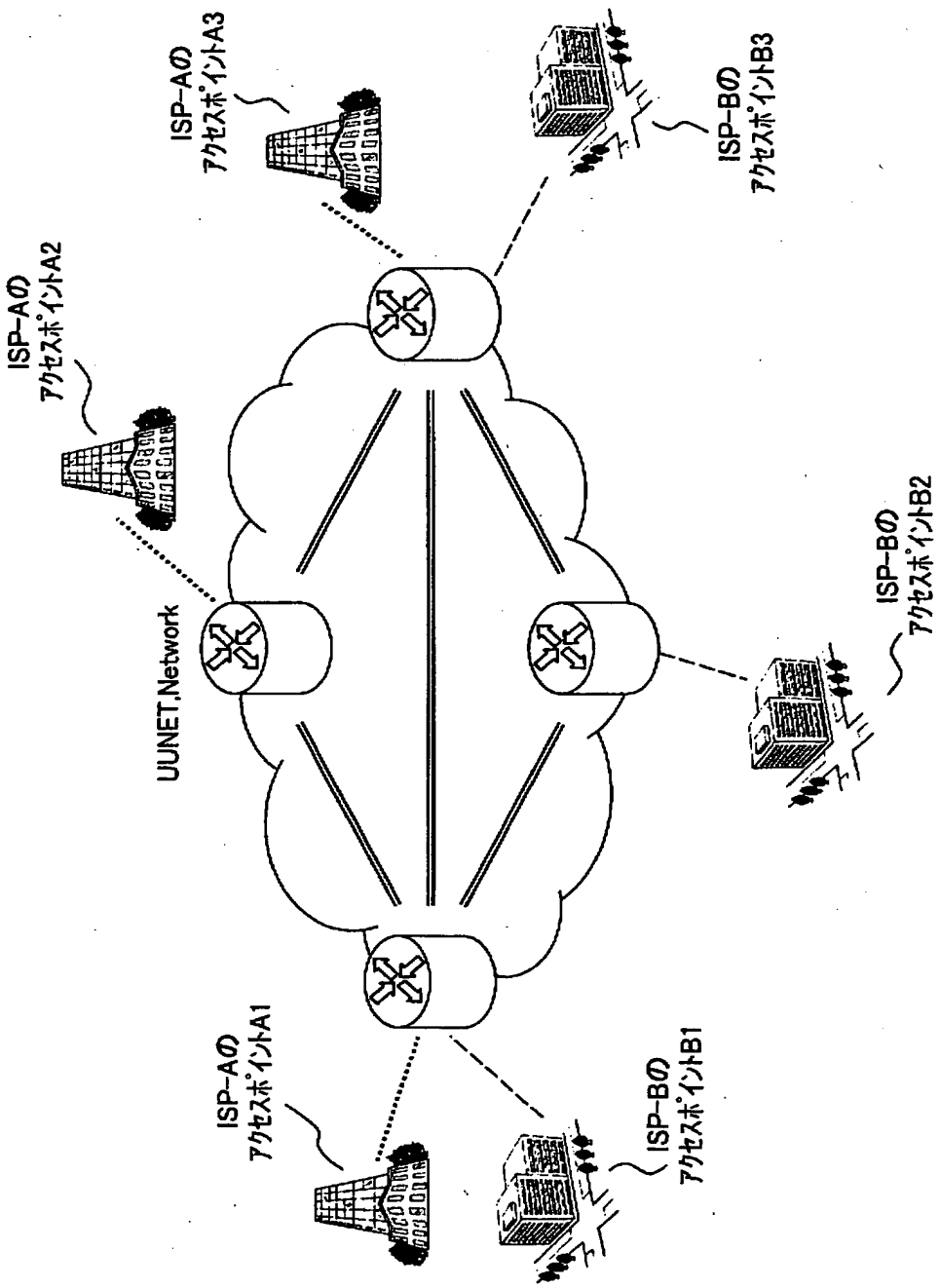
【図１１】

仮想私設網の構築例(その1)



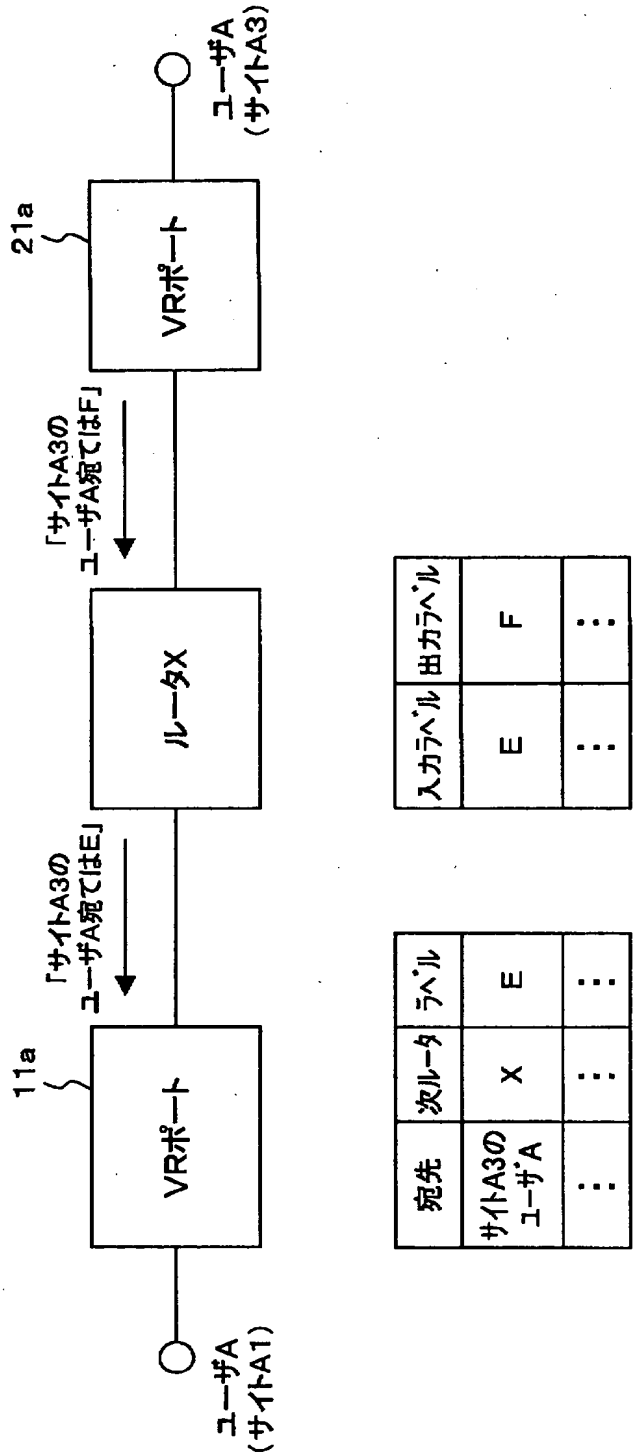
【図１２】

仮想私設網の構築例(その2)



【図１３】

VRポート間でラベルパスを設定する手順の例



【書類名】　　要約書

【要約】

【課題】　ＩＰ網を利用した仮想私設網のセキュリティを向上させる。

【解決手段】　ルータ装置は、仮想私設網サービスのユーザ毎にＶＲポート３０を備える。各ＶＲポート３０は、それぞれ対応する仮想私設網のためのルーティングテーブル３２を有している。制御チャネル終端部３３およびＶＰＮ構成モジュール３５は、同一の仮想私設網に属するＶＲポートとの間にＬ２ＴＰトンネルを設定する。ゲートウェイプロトコルデーモン３１は、設定されたＬ２ＴＰトンネルを介してルーティング情報を交換し、ルーティングテーブル３２を作成／更新する。入力されたパケットは、ルーティングテーブル３２に従ってルーティングされる。

【選択図】　図５

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社